HYBRID-ARQ AS A COMMUNICATIONS SECURITY MEASURE

Sandipan Kundu, Dimitris A. Pados†, and Stella N. Batalama

Department of Electrical Engineering, State University of New York at Buffalo, NY 14260
E-mail: {skundu,pados,batalama}@buffalo.edu

ABSTRACT

We consider arbitrary Hybrid-Automatic-Repeat-Request (H-ARQ) wireless links over quasi-static Rayleigh fading channels. In this paper, we translate the repeat-request advantage of the intended receiver over potential eavesdroppers to link security. In particular, with statistical-only knowledge of the channel and noise, we find for the first time in the literature the optimal power allocation sequence over the H-ARQ rounds that maximizes the outage probability of eavesdroppers for any given target outage probability of the trusted receiver. Simulation studies demonstrate orders of magnitude difference in outage probability between eavesdroppers and intended receiver.

Index Terms— Eavesdropping, hybrid-ARQ, physical-layer security, power allocation, SISO wiretap channel.

1. INTRODUCTION

In [1], Wyner explained that secure communication between two terminals is possible if the eavesdropper's channel is a degraded version of the channel of the intended receiver. Motivated by [1], information-theoretic secrecy capacity analysis has been carried out for various communication setups [2]-[13]. In particular, secrecy under joint channel coding and automatic-repeat-request (ARQ) operation was studied in [14], [15]. Signal processing research has attempted to materialize -at least partly- the information theoretic secrecy capacity promises [16]-[22]. The works in [16]-[20] guaranteed a certain Quality-of-Service (QoS) at the trusted receiver and suppressed the useful information content in the received signal of the eavesdropper by: (i) Beamforming designs that utilize the spatial degrees of freedom available in multi-antenna systems and (ii) artificial-noise aided methods (with or without instantaneous channel state information of the eavesdropper). Waveform-design based security for the common multipath single-input single-output (SISO) channel was developed in [21],[22].

When spatial and time-domain degrees of freedom are not available, none of the methods in [16]-[20] or [21],[22] is applicable. We can still, however, enhance significantly data-link security by installing a security-optimized Hybrid-Automatic-Repeat-Request (H-ARQ) protocol that takes advantage of the fact that only intended recipients can request re-transmissions. In this paper, for the first time in the literature, we optimize L-round H-ARQ transmission protocols for the transmitter-to-trusted-receiver pair. We assume that the transmitter-to-trusted-receiver and transmitter-to-eavesdropper-receiver channels experience quasi-static Rayleigh fading, i.e. channels do not change significantly during re-transmissions of the same information packet and may change independently when transmitting a new information packet. Only statistical knowledge of the channel and noise power is assumed available for our secure H-ARQ protocol design. With this knowledge, we find offline the optimal power allocation sequence over the H-ARQ rounds that maximizes the outage probability of the eavesdropper for any given outage probability requirement for the trusted receiver. The developed secure H-ARQ data link can be installed directly on top of physical-layer security solutions of [16]-[20] (antenna-array techniques) and/or [21], [22] (waveform design).

2. SYSTEM MODEL

We consider an ($L>1$)-round H-ARQ protocol for a transmitter (Alice) and a trusted receiver (Bob) in the presence of an eavesdropper (Eve) where each is equipped a with single transmit/receive antenna. The H-ARQ transmission scheme operates as follows. First, Alice (source) transmits a data packet to Bob (trusted receiver) which is overheard by Eve (eavesdropper). Upon reception of the transmitted data packet, Bob indicates success or failure of receiving the packet by feeding back a single bit of acknowledgement (ACK) or negative acknowledgement (NACK), respectively, to Alice through a separate errorless Bob-to-Alice feedback channel. Bob-to-Alice feedbacks are error-free overheard by Eve as well. If a NACK is received by Alice and the maximum number of re-transmissions L allowed by the protocol has not been reached, Alice re-transmits the packet with potentially different transmission power (to be optimized under some design criterion). If ACK is received by Alice or the maximum allowable re-transmission is reached, Alice starts transmitting a new data packet. In each re-transmission round, both Bob and Eve attempt to decode the transmitted data packet by combining received data from all previous re-transmission rounds of the same data packet via maximal-ratio-combining (MRC). If Bob cannot decode a data packet after L re-transmission rounds, then Bob records an outage for the data packet. In other words, the accumulated signal-to-

†Corresponding author.

noise ratio (SNR) of the combined received packet at Bob is below a target preset required SNR threshold. It is intriguing to investigate the frequency of outage events for Eve, since Eve does not have the benefit of requesting re-transmissions.

Given the maximum number of allowable re-transmission rounds L for the H-ARQ protocol, the received signal at Bob/Eve (subscript B/E) at the lth re-transmission round is given by

$$y_{B/E}^{l} = \sqrt{P_l} h_{B/E}\, x + n_{B/E},\ l = 1, \cdots, L, \tag{1}$$

where P_l is the transmitted power in the lth H-ARQ round, x is a unit-power transmitted data packet, $h_{B/E}$ are the channel coefficients between Alice and Bob/Eve, respectively, and $n_{B/E}$ is additive noise at Bob/Eve. The channel coefficients $h_{B/E}$ are modeled as complex Gaussian random variables with mean zero and variance (power) $\sigma_{B/E}^2 \triangleq R_{B/E}^{-\omega_{B/E}}$ where $R_{B/E}$ is the distance between Alice and Bob/Eve and $\omega_{B/E}$ is the path loss exponent. The channels are assumed to be quasi-static, i.e. the channel does not change during re-transmissions of the same data packet and it may change independently when a new data packet is transmitted. The channel coefficient h_B is assumed to be known at Bob for coherent data reception. Similarly, the channel coefficient h_E is known to Eve who also has error-free access to the ACK/NACK Bob-to-Alice feedback channel (worst case security scenario). This allows Eve to perform MRC decoding as well on the received data packets from the H-ARQ re-transmissions. The noise $n_{B/E}$ at Bob/Eve is modeled as additive white Gaussian with mean zero and variance $N_{B/E}$.

Bob combines the received data packets from all previous re-transmission rounds and jointly decodes the data packet with accumulated signal-to-noise ratio (SNR) after l ($1 \le l \le L$) re-transmission rounds equal to

$$\mathbb{SNR}_B^l = \frac{\sum_{i=1}^{l} P_i |h_B|^2}{N_B}. \tag{2}$$

Similar to Bob, the accumulated SNR at Eve after l ($1 \le l \le L$) re-transmission rounds is

$$\mathbb{SNR}_E^l = \frac{\sum_{i=1}^{l} P_i |h_E|^2}{N_E}. \tag{3}$$

3. OUTAGE PROBABILITY AND PROBLEM FORMULATION

The probability of the event that the accumulated SNR of Bob/Eve after l re-transmission rounds is below a given target SNR threshold γ_0 is given by[1]

$$p_{B/E}^{out,l} = \Pr[\mathbb{SNR}_{B/E}^l < \gamma_0] = 1 - e^{-\frac{\gamma_{B/E}}{\sum_{i=1}^{l} P_i}} \tag{4}$$

where $\gamma_{B/E} = \frac{\gamma_0 N_{B/E}}{\sigma_{B/E}^2}$ and $\Pr[\cdot]$ denotes event probability.

The probability of the event that the H-ARQ protocol between Alice and Bob stops successfully exactly after l rounds of re-transmissions, i.e. Bob's accumulated SNR after $l-1$ rounds is below the target SNR threshold γ_0 and Bob's accumulated SNR after l rounds is above the target SNR threshold, is given by

$$p_B^{stop,l} = p_B^{out,l-1} - p_B^{out,l} = e^{-\frac{\gamma_B}{\sum_{i=1}^{l-1} P_i}} - e^{-\frac{\gamma_B}{\sum_{i=1}^{l} P_i}}. \tag{5}$$

3.1. Outage probability of Bob

An outage event for Bob can happen only when all L rounds of re-transmission are executed and still the accumulated SNR at Bob fails to meet the target SNR threshold for successful decoding of the data packet. Hence, the probability of an outage event for Bob is given simply by (4) for $l = L$, i.e.

$$P_{out}^B = p_B^{out,L} = 1 - e^{-\frac{\gamma_B}{\sum_{i=1}^{L} P_i}}. \tag{6}$$

3.2. Outage probability of Eve

Eve's outage event will depend not only on her own channel condition, but also on how many re-transmissions between Alice and Bob occurred, which is not under her control. In detail, Eve will have outage if: *(i)* after the lth H-ARQ round Eve's SNR is below the target SNR threshold and Bob's SNR is above and Bob's SNR was below the target SNR threshold after the $(l-1)$th H-ARQ round or *(ii)* when Eve's SNR is below the target SNR threshold after L H-ARQ rounds and Bob's SNR is below the target SNR threshold after $(L-1)$ H-ARQ rounds. Thus, the outage probability for Eve for an $L \ge 3$ H-ARQ protocol between Alice and Bob is given by

$$\begin{aligned} P_{out}^E &= \left(1 - e^{\frac{-\gamma_E}{P_1}}\right)\left(e^{\frac{-\gamma_B}{P_1}}\right) \\ &+ \sum_{l=2}^{L-1}\left(1 - e^{\frac{-\gamma_E}{P_1+\cdots+P_l}}\right)\left(e^{\frac{-\gamma_B}{P_1+\cdots+P_l}} - e^{\frac{-\gamma_B}{P_1+\cdots+P_{l-1}}}\right) \\ &+ \left(1 - e^{\frac{-\gamma_E}{P_1+\cdots+P_L}}\right)\left(1 - e^{\frac{-\gamma_B}{P_1+\cdots+P_{L-1}}}\right). \end{aligned} \tag{7}$$

For the special case of a H-ARQ protocol of two rounds ($L = 2$), the outage probability for Eve is given by

$$P_{out}^E = \left(1 - e^{\frac{-\gamma_E}{P_1}}\right)\left(e^{\frac{-\gamma_B}{P_1}}\right) + \left(1 - e^{\frac{-\gamma_E}{P_1+P_2}}\right)\left(1 - e^{\frac{-\gamma_B}{P_1}}\right). \tag{8}$$

When $L = 1$ (no re-transmissions), the outage probability for Eve is

$$P_{out}^E = 1 - e^{\frac{-\gamma_E}{P_1}}, \tag{9}$$

which is of course the same as Bob's (if γ_E=γ_B) since no H-ARQ is implemented.

Our goal now in this paper is to find the optimal power allocation for the $L > 1$ rounds of a H-ARQ protocol that under a target outage probability of Bob (for reliable transmission) maximizes the outage probability of Eve (for secure transmission). For a H-ARQ protocol with Bob's targeted outage probability ρ_0, the problem of finding the optimal power assignment takes the form

$$\begin{aligned} \arg\max_{P_1,\cdots,P_L} \quad & P_{out}^E && \text{(10a)} \\ \text{subject to} \quad & P_{out}^B \le \rho_0, && \text{(10b)} \\ & P_l \ge 0,\ l = 1, \cdots, L, && \text{(10c)} \end{aligned}$$

[1] We assume that the same SNR threshold γ_0 is required by both Bob and Eve for successful packet decoding.

where P_{out}^B and P_{out}^E are given by (6) and (7), (8), respectively.

4. OPTIMAL POWER ALLOCATION

Bob's outage probability constraint in (10b) implies that, with a targeted SNR γ_0, the outage probability of the H-ARQ protocol with L transmissions should not be larger than the specified outage probability constraint ρ_0 or

$$\begin{aligned} P_{out}^B &= 1 - e^{-\frac{\gamma_B}{\sum_{i=1}^L P_i}} \leq \rho_0 \\ &\Rightarrow \quad P_1 + \cdots + P_L \geq \frac{\gamma_B}{\ln\frac{1}{1-\rho_0}} \triangleq P_0. \end{aligned} \tag{11}$$

It can be shown easily that at the optimal point of problem (10), constraint (10b) or (11) is satisfied with equality. We move, now, one step away from (10) and relax the non-negative condition (10c) on the H-ARQ transmission power values per round, $P_l = 1, 2, \cdots, L$. The re-formulated *relaxed* problem is

$$\begin{aligned} \arg\max_{P_1,\cdots,P_L} \quad & P_{out}^E && \text{(12a)} \\ \text{subject to} \quad & P_1 + \cdots + P_L = P_0 && \text{(12b)} \\ & P_l \in \mathbb{R},\ l = 1, \cdots, L. && \text{(12c)} \end{aligned}$$

The Lagrange function of the *relaxed* version of problem (10) with Lagrange multiplier λ can be written as

$$\mathcal{L}(P_1, \cdots, P_L, \lambda) = P_{out}^E + \lambda\Big(P_1 + \cdots + P_L - P_0\Big). \tag{13}$$

Taking partial derivatives of (13) with respect to λ and P_l, $l = 1, \cdots, L$, and setting them to zero, we obtain the $L + 1$ equations

$$\begin{aligned} \frac{\partial \mathcal{L}}{\partial P_l} &= 0,\ l = 1, \cdots, L, && \text{(14)} \\ P_1 + \cdots + P_L &= P_0. && \text{(15)} \end{aligned}$$

The L power values that solve the Lagrangian equations are as follows[2]

$$P_2 = \frac{P_1^2 \log\{\frac{\gamma_B+\gamma_E}{\gamma_B}\}}{\gamma_E - P_1 \log\{\frac{\gamma_B+\gamma_E}{\gamma_B}\}}, \tag{16}$$

$$P_k = \frac{(P_1 + \cdots + P_{k-1})^2 \log\{G_k\}}{\gamma_E - (P_1 + \cdots + P_{k-1}) \log\{G_k\}} \tag{17}$$

where

$$G_k = \frac{\gamma_B + \gamma_E\left\{1 - e^{-\frac{\gamma_B P_{k-1}}{(P_1+\cdots+P_{k-1})(P_1+\cdots+P_{k-2})}}\right\}}{\gamma_B} \tag{18}$$

for $k = 3, \cdots, L$ and

$$P_1 = P_0 - (P_2 + \cdots + P_L). \tag{19}$$

[2]Details of partial derivative and P_l, $l = 1, \cdots, L$, computations are omitted due to space limitations.

The solution given by (16)-(19) solves the *relaxed* optimization problem in (12a)-(12c) and might be infeasible (negative power values) for the original optimization problem in (10a)-(10c). If, however, we can prove that the L optimal power values returned by (16)-(19) are always non-negative, then the obtained solution will also be the optimal solution for the problem in (10a)-(10c). We use the following two lemmas to prove that the obtained power values are indeed positive. The proofs of the lemmas themselves are omitted due to lack of space.

Lemma 1 *For fixed γ_B, γ_E, G_k, $k = 3, \cdots, L$, are independent of the transmitted power in the H-ARQ rounds and given recursively by*

$$G_2 = \frac{\gamma_B + \gamma_E}{\gamma_B}, \tag{20}$$

$$G_k = \frac{\gamma_B + \gamma_E\Big(1 - e^{\frac{-\gamma_B log\{G_{k-1}\}}{\gamma_E}}\Big)}{\gamma_B}, \tag{21}$$

for $k = 3, \cdots, L$. □

Having all constants G_k, $1 < k \leq L$, calculated recursively by (20) and (21) means that all power values can also be recursively computed by (16), (17) given power value P_1. We seek now the power value P_1 that satisfies the Lagrange solution (16)-(19).

Lemma 2 *For given γ_B, γ_E and $G_2, \cdots, G_L$ calculated by (20), (21), the first-round power value*

$$P_1 = \frac{P_0\, \gamma_E}{\gamma_E + P_0\, log\{G_2 G_3 \cdots G_L\}} \tag{22}$$

satisfies (16)-(19) with all-round total power $P_0 = \frac{\gamma_B}{ln\frac{1}{1-\rho_0}}$ as defined in (11). □

By (22), (16), and (17), we solved in closed recursive form the problem in (12a)-(12c). In the sequel, we investigate the sign of P_k, $k = 1, \cdots, L$. By (22), $0 < P_1 < \frac{\gamma_E}{\log\{G_2 \cdots G_L\}}$. Assume $P_2, \cdots, P_{k-1}$ are all non-negative. Then, from (17) P_k is non-negative if

$$P_1 + \cdots + P_{k-1} < \frac{\gamma_E}{\log\{G_k\}} \tag{23}$$

$$\text{or } \frac{\gamma_E\, P_1}{\gamma_E - P_1 \log\{G_2 \cdots G_{k-1}\}} < \frac{\gamma_E}{\log\{G_k\}}$$

$$\text{or } P_1 < \frac{\gamma_E}{\log\{G_2 \cdots G_k\}}, \tag{24}$$

which is true. Formally, we conclude that (22), (16), and (17) present us with a *unique stationary solution point* of (10a)-(10c). Technically, we still need to establish that the found stationary point is the maximizer and not the minimizer. It is easy to check that the outage probability of Eve with power allocation $P_1 = P_0, P_2 = 0, \cdots, P_L = 0$ is smaller than the outage probability of Eve with power allocation given by the solution of the Lagrangian equations, which completes the proof. For ease in reference, we summarize the complete H-ARQ power calculation procedure in Table I.

Table 1. Secure L-round H-ARQ power allocation sequence

Step 1: Input: Successful-decoding SNR threshold γ_0;
Bob's outage probability threshold ρ_0;
channel power values $\sigma^2_{B/E}$;
noise variance values $N_{B/E}$.

Step 2: Calculate: $P_0 = \frac{\gamma_B}{\ln\frac{1}{1-\rho_0}}$, $\gamma_B = \frac{\gamma_0 N_B}{\sigma^2_B}$, $\gamma_E = \frac{\gamma_0 N_E}{\sigma^2_E}$,

$G_2 = \frac{(\gamma_B+\gamma_E)}{\gamma_B}$,

$G_k = \frac{\gamma_B+\gamma_E\left(1-e^{\frac{-\gamma_B \log\{G_{k-1}\}}{\gamma_E}}\right)}{\gamma_B}$ for $k = 3, \cdots, L$.

Step 3: Optimal power allocation:

$P_1^* = \frac{\gamma_E P_0}{\gamma_E + P_0 \log\{G_2 \cdots G_L\}}$,

$P_k^* = \frac{(P_1+\cdots+P_{k-1})^2 \log\{G_k\}}{\gamma_E - (P_1+\cdots+P_{k-1}) \log\{G_k\}}$ for $k = 2, \cdots, L$.

Step 4: Output: $P_1^*, \cdots, P_L^*$ (globally optimal solution).

5. SIMULATION RESULTS

First, in Fig. 1 we validate by simulations the theoretically derived outage probability of Bob and Eve as a function of the required SNR threshold for an H-ARQ protocol with $L = 8$ rounds and fixed equal transmission power per round. Equal distance from Alice is assumed, $R_B = R_E = 1$, and the path loss coefficients are set to $\omega_B = \omega_E = 2$. Certainly, perfect match is observed between analytical and simulation estimated probability values. For the same experimental set-up, in Fig. 2 we plot the outage probability of Eve as we vary the number of H-ARQ rounds. The outage probability requirement on Bob is set to 10^{-4} with decoding SNR threshold 12 dB. With $R_B = R_E = 1$, conventional equal power allocation provides some nominal security, but optimal power allocation pushes the outage probability of Eve to nearly 0.5. As we increase the distance between Alice and Bob relative to Eve, the outage probability of Eve improves and becomes easily comparable to Bob's under equal power allocation. Still, security-optimal power allocation maintains orders-of-magnitude outage probability advantage for Bob even when his channel faces a 10-fold distance disadvantage compared to Eve. A short H-ARQ of $L = 2$ or 3 rounds is enough to reap security benefits under power allocation optimization.

As a final -somewhat extreme- study, in Fig. 3 we plot the outage probability of Eve under equal and optimal power allocation ($L = 2, 5$, or 10 rounds) as we vary the distance between Alice and Bob from five to fifty times the distance between Alice and Eve. The study shows that *(i)* equal power allocation affords no security and *(ii)* optimal power allocation results to one order of magnitude outage probability disadvantage to Eve even when Bob is 35 times further away from Alice than Eve is. Even under the extreme case where $R_B = 50$ and $R_E = 1$ and the channel power of Bob is 250 times worse than Eve ($\omega_{B/E} = 2$), optimal power allocation was able to keep the outage probability of Eve above Bob's guaranteed outage probability of 10^{-4}.

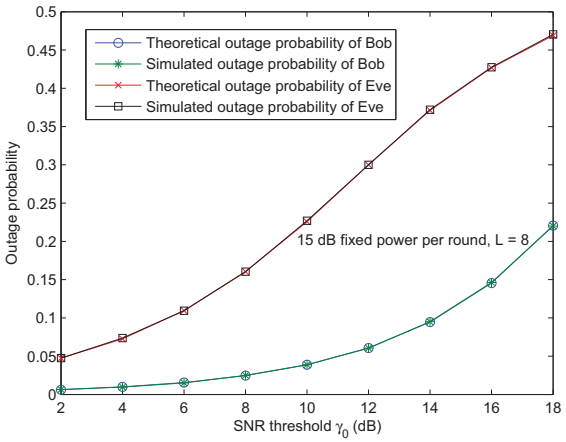

Fig. 1. Outage probability validation vs SNR threshold γ_0 ($L = 8$, fixed 15 dB transmission power per round.)

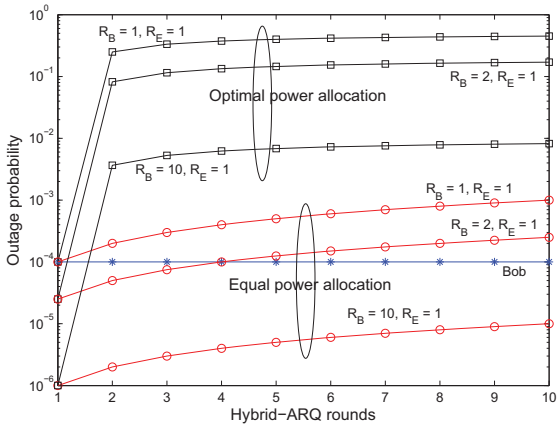

Fig. 2. Outage probability of Eve vs H-ARQ rounds (outage probability of Bob $\rho_0 = 10^{-4}$, SNR threshold $\gamma_0 = 12$ dB.)

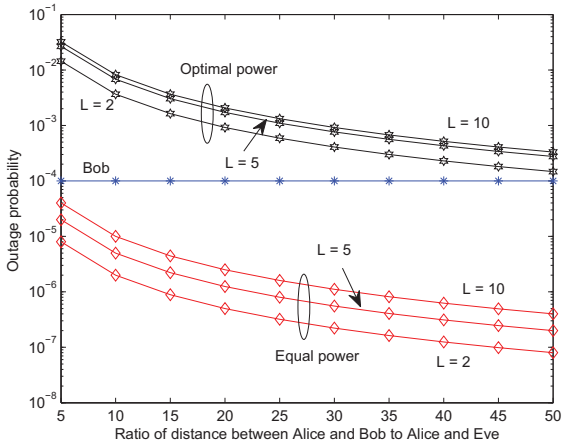

Fig. 3. Outage probability of Eve vs relative Alice-to-Bob to Alice-to-Eve distance ($\rho_0 = 10^{-4}$, $\gamma_0 = 10$ dB).

6. REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Intern. Symp. Inf. Th.*, Seattle, WA, July 2006, pp. 356–360.

[3] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2470–2492, June 2008.

[4] Z. Li, R. D. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE Intern. Symp. Inf. Th.*, Nice, France, June 2007, pp. 1296–1300.

[5] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[6] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[7] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2453–2469, June 2008.

[8] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Intern. Symp. Inf. Th.*, June 2007, Nice, France, pp. 2471–2475.

[9] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Intern. Symp. Inf. Th.*, July 2008, Toronto, Canada, pp. 524–528.

[10] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," in *Proc. IEEE Intern. Symp. Inf. Th.*, June 2009, Seoul, Korea, pp. 2602–2606.

[11] S. Shafiee and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 4033–4039, Sept. 2009.

[12] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Intern. Symp. Inf. Th.*, Adelaide, Australia, Sept. 2005, pp. 2152–2155.

[13] J. Li, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 1176–1187, Apr. 2011.

[14] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, pp. 1575–1591, Apr. 2009.

[15] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: a security gap analysis," *IEEE Trans. Inf. Forens. Security*, vol. 7, pp. 883–894, June 2012.

[16] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I:The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 3088–3104, July 2010.

[17] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 5515–5532, Nov. 2010.

[18] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, June 2008.

[19] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. of IEEE Intern. Conf. Acoust., Speech, and Signal Proc.*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[20] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Proc.*, vol. 59, pp. 1202–1216, Mar. 2011.

[21] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE J. Sel. Areas Commun.*, Special Issue on Signal Proc. Techn. for Wireless Phys. Layer Security, vol. 31, pp. 1864–1874, Sept. 2013.

[22] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Secure waveforms for SISO channels," in *Proc. IEEE Intern. Conf. Acoust., Speech, and Signal Proc.*, Vancouver, Canada, May 2013, pp. 4713–4717.